EAR Fact Sheet

# Securing Vehicle-to-Vehicle Communication through Consortium Blockchain

Exploratory Advanced Research...Next Generation Transportation Solutions

Source: USDOT.

Vehicle-to-vehicle (V2V) communication uses wireless technology to send and receive messages with surrounding vehicles. V2V communication increases highway safety through precollision warnings and provides convenience, such as information on traffic congestion. It is becoming standard in the automotive trade to install equipment on new vehicles that allow V2V communication. One concern in wireless communication is the increasing potential for unauthorized intrusions or cyberattacks, along with breech of personal privacy. The Federal Highway Administration's (FHWA's) Exploratory Advanced Research (EAR) Program is supporting a project to research and develop software that increases V2V security by improving upon the current "handshake" protocols for authenticating vehicle identification, along with maintaining security during message transportation. Researchers at the New Jersey Institute of Technology are conducting the research project, "Decentralized Vehicle Credential Management System Based on Consortium Blockchain."

## The Need to Address Current Standards in V2V Communication

Current V2V communication relies on a centralized certificate authority (CA) to authenticate vehicle identity, thus creating a "trust" or handshake between two vehicles. The CA issues a certificate, which verifies a vehicle's identity as being accurate and valid. Certificates allow both parties to establish a secure and encrypted channel for communication. But there is cause for concern. First, identity leaks can occur during the CA connection process before authentication. It is possible to intercept transmissions, much like your neighbor using your unsecured wireless internet connection.

"A breach could, in theory, lead to the attacker gaining access to the identity of an owner/operator and certificates for a specific vehicle. The access to certificates would theoretically allow tracking of a vehicle," said Volker Fessmann, FHWA's Research Transportation Specialist.

A second, more critical issue occurs when the CA itself is compromised. Sometimes referred to as man-in-the-middle, this intrusion results from some unauthorized entity hacking into and assuming the identity of the CA. The intruder then issues a certificate on behalf of the CA, thereby creating a three-way channel between vehicles and the CA imposter.

The project team aims to research and develop software that addresses cybersecurity concerns by meeting the following demands:

- *Authenticity and integrity*. V2V communications must be conducted over secure channels, using cryptographic protocols to authenticate vehicle identity and secure message transmissions.
- *Vehicle anonymity*. There must be a break in the link between a vehicle's actual identity and the authentication process. One possible solution is to replace vehicle identity with pseudonyms. The pseudonym must be bound to the vehicle's real identity without leaking the real identity during the authentication process.
- *Nonequivocating vehicle identities*. Authentication must occur from a system that cannot be compromised, biased, or interrupted by unauthorized sources. Properly implemented, consortium blockchain mitigates these risks.

## The Basics of Consortium Blockchain

Blockchain technology originated in 2008 as a distributed ledger technology recording Bitcoin transactions. Essentially, blocks of transactions are chained together, each containing a randomly generated number unique to the block, an encrypted 256-bit "hash" that consists of data unique to the block plus data from the previous block's hash, a timestamp, and the transaction. Therefore, altering a block of information requires alteration of each subsequent block.

No one computer or organization can own the chain. Identical copies of the chain exist across many computers in many organizations. Each chain participant stores an exact copy of the chain. When a request to add a new block occurs, algorithms poll chain participants to verify that the new block's data match existing copies across the chain. Only after a consensus of participants confirm data integrity can the new block join the chain.

Blockchains can be public, private, or consortium. Anyone can access public chains, while private chains exist within a controlled environment with limited access and one organization assuming ownership. Consortium blockchain combines the two where access is limited to specific users and ownership is spread across different organizations within the consortium group.

U.S. Department of Transportation
Federal Highway Administration

# Securing Vehicle-to-Vehicle Communication through Consortium Blockchain

## Steps to Achieving Advanced Cryptographic Security

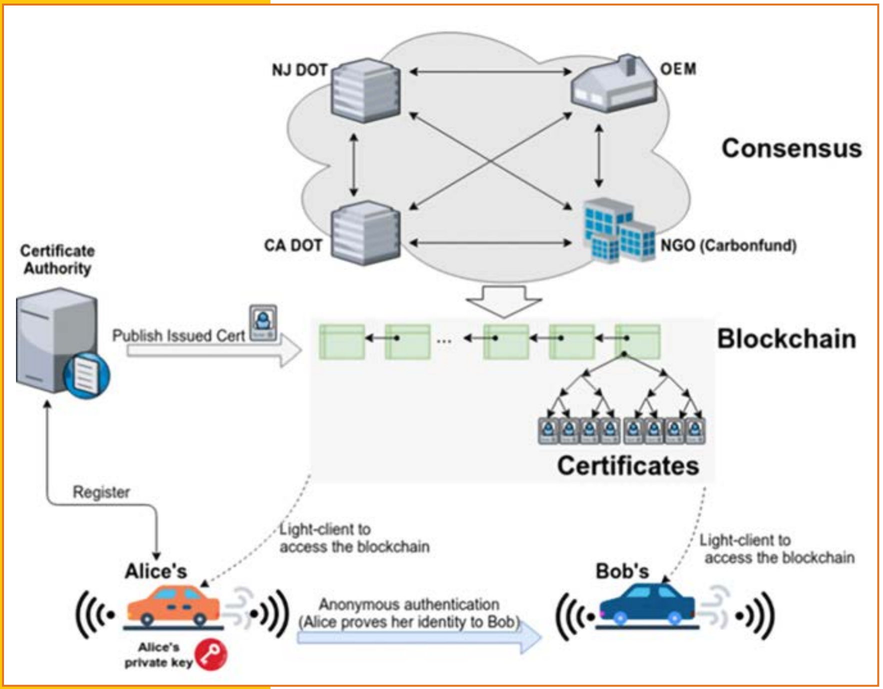
The researchers began work on the 3-year project in September 2020. Currently in the first segment of the project, the team is researching literature on consensus protocols.

In the second segment, they will develop a high-performing consortium blockchain. As most blockchain is open source, the team will begin by surveying existing blockchain protocols. After customizing code to meet the needs of V2V communication, the researchers will implement blockchain in a cloud environment. With security and bug fixes complete, the team will move to the second phase of this segment, using the blockchain to implement a decentralized credential management system.

In the third segment, the team will develop and implement a decentralized anonymous credential system based on the blockchain. The system allows for the blacklisting of invalid vehicle identities. In this way, vehicles can check the blacklist for invalid certificates before accessing the blockchain.

In the last segment, the team will develop and implement a lightweight software package that will allow vehicles to anonymously and securely access the blockchain. Before authentication, the software self-mints a pseudonym certificate based on the actual digital certificate issued to the vehicle, maintaining its real identity throughout the authentication and communication process.

The project's final leg is to make code packages for an anonymous decentralized credential management system available. Code packages, for example, could be placed on the U.S. Department of Transportation's Intelligent Transportation Systems (ITS) CodeHub website (https://its.dot.gov/code), a repository for open-source, reusable ITS code. The CodeHub site allows researchers and developers to share their innovations that may one day make highways and roadways safer for all.



©2021 New Jersey Institute of Technology.

EXPLORATORY ADVANCED RESEARCH

## What Is the EAR Program?

The EAR Program addresses the need for longer term, higher risk research with the potential for transformative improvements to transportation systems. The EAR Program seeks to leverage advances in science and engineering that could lead to breakthroughs for critical, current, and emerging issues in highway transportation by experts from different disciplines who have the talent and interest in researching solutions and might not do so without EAR Program funding.

To learn more about the EAR Program, visit https://highways.dot.gov/research/exploratory-advanced-research. The website features information on research solicitations, updates on ongoing research, links to published materials, summaries of past EAR Program events, and details on upcoming events.

## Learn More

For more information about this EAR Program project, contact Govindarajan Vadakpat, *FHWA Office of Operations Research and Development*, at **202-493-3283** (email: g.vadakpat@dot.gov).

Recommended citation: Federal Highway Administration, Securing Vehicle-to-Vehicle Communication through Consortium Blockchain (Washington, DC: 2021) https://doi.org/10.21949/1521646